工程科学学报，第 37 卷，第 9 期：1225－1229，2015 年 9 月
Chinese Journal of Engineering，Vol. 37，No. 9：1225－1229，September 2015
DOI：10.13374/j.issn2095－9389.2015.09.017；http://journals.ustb.edu.cn

基于模糊保险箱的人脸－人耳融合模板保护

袁　立✉，李文明

北京科技大学自动化学院，北京 100083
✉ 通信作者，E-mail：lyuan@ustb.edu.cn

摘　要　鉴于人脸与人耳两种生物特征在图像获取上的相似性以及生理位置上的互补性，提出一种人脸－人耳多模态融合模板保护方法，将两者在特征层进行融合，然后利用模糊保险箱算法对融合模板进行保护．该方案基本流程分为五部分：图像预处理、Gabor－PCA 特征提取、特征融合、融合模板加密以及融合模板解密．在由 ORL 人脸库和 USTB 人耳库 3 构成的人脸－人耳多模态图像库上的认证实验结果表明所提模板防护方法的有效性，且基于融合模板保护的认证结果比基于单模板保护的认证结果在识别率和误识率上均有所优化．

关键词　生物特征模板保护；模式识别；特征提取；信息融合；模糊保险箱
分类号　TP391.4

Face and ear fusion template protection based on fuzzy vaults

YUAN Li✉，*LI Wen-ming*

School of Automation and Electrical Engineering，University of Science and Technology Beijing，Beijing 100083，China
✉ Corresponding author，E-mail：lyuan@ustb.edu.cn

ABSTRACT　Due to biological characteristic similarity in image acquisition and physiological complementarity of the face and the ear，a face and ear multimodal fusion template protection method was proposed，in which the face and the ear were combined in the feature level and then a fuzzy vault was utilized to protect the fusion feature template. The basic flow of the scheme was divided into 5 parts：image preprocessing，Gabor－PCA feature extraction，feature fusion，fusion template encryption，and fusion template decryption. On the multimodal image dataset consisted of the ORL face dataset and the USTB ear dataset 3，authentication experimental results show the effectiveness of the proposed fusion template protection method. Also the fusion template protection method outperforms the unimodal template protection method on both genuine accept rate and false accept rate.

KEY WORDS　biometric template protection；pattern recognition；feature extraction；information fusion；fuzzy vaults

随着网络技术和信息技术的不断发展，电子商务、政务和网上办公等越来越多的领域需要可靠的身份识别．生物特征识别技术在身份认证中的应用逐渐增多，但是也暴露出其本身所固有的一些安全性和隐私性方面的缺陷．因此，对生物特征模板的保护有了更高的要求，并成为生物特征识别领域的一个研究热点．生物特征模板保护可分为两类[1]：基于变换的方法和基于密钥的方法．前者包括双因子认证和不可逆变换，该方法是通过变换，将生物特征模板转换成随机模板，然后使用随机模板进行验证；后者使用的方法是结合密钥和生物特征对用户进行验证．基于密钥的方法主要有密钥释放、密钥绑定和密钥生成．密钥释放的方法是将密钥和生物特征简单的叠加在一起，存储为加密的生物特征模板；密钥绑定是将生物特征模板和密钥按照一定的方法结合起来，只有当生物特征匹配成功时，密钥才能提取出来；密钥生成是从生物特征中提取出一个密钥，而不是从外部输入．模糊保险箱（fuzzy vault）[2]算法是密钥绑定中比较经典的算法，分为加密和解密两个步骤[3－4]．在加密阶段，将注册生物特征模板与密钥结合，生成保险箱；在解密阶段，使

收稿日期：2014－06－03

用待认证生物特征模板来提取密钥，如果与已注册的生物特征模板一致，则会得到正确的密钥，从而实现认证.

为了保持人脸认证所具有的非打扰式的特点，并鉴于人脸与人耳两种生物特征在图像获取上的相似性以及生理位置上互补性[7]，将人脸与人耳生物特征相结合进行身份认证，在一定程度上解决人脸认证中受姿态、年龄、表情等因素的影响. 在认证过程中，利用模糊保险箱算法对人脸—人耳融合特征模板进行保护. 图 1 所示为系统结构图. 本系统分为注册和认证两个阶段. 在注册阶段，首先利用 Gabor 滤波器分别对人脸和人耳注册图像进行 Gabor 变换，然后利用主元分析法对 Gabor 特征进行降维，由于人脸和人耳特征模板是同质的，所以可以将两者进行特征层融合，生成融合特征模板. 接下来，利用模糊保险箱算法对融合模板进行加密，并将结果存储在保险箱 V 中. 在认证阶段，将待认证的人脸图像和人耳图像经过 Gabor 变换和主元分析特征提取后进行特征层融合，然后将融合模板与模糊保险箱中的数据进行比较，最终输出匹配结果：释放密钥或是提示认证失败.

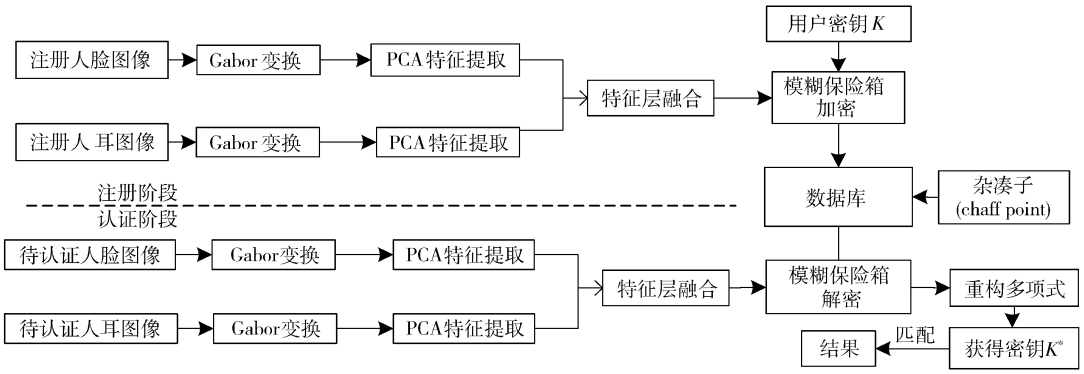

图 1　基于模糊保险箱算法的多特征融合的生物特征模板保护系统框图

Fig. 1　Multimodal template protection system diagram based on data transformation and fuzzy vaults

1　保护策略

利用模糊保险箱对生物特征模板进行保护时分为加密和解密两个阶段. 加密过程的主要作用是将注册生物特征模板利用密钥进行转换形成真实点集，并与添加的杂凑点集共同构成保险箱；解密过程的主要作用是将待认证生物特征模板通过保险箱提取密钥，当释放出正确密钥时，则表明待认证模板与注册模板一致，从而得到认证结果.

1.1　加密过程

模糊保险箱算法定义在有限域 F 上. 在加密阶段，选择关于 x 的多项式 p 来加密密钥 K，然后计算注册生物特征模板 s 在多项式 p 上的投影 $p(s)$，这样 $(s, p(s))$ 就构成了一个有限点集，即为真实点集. 接下来随机生成一个杂凑点集，与真实点集一起构成一个数据集合 V，即是保险箱. 在 V 中，杂凑点的数量要远远大于真实点的数量. 模板加密过程的具体流程如图 2 所示，具体步骤如下所述.

(1) 对密钥 K 进行 CRC 循环冗余校验编码[8]. 密钥是一组随机生成的 128 位的二进制密钥 K，采用 CRC—16 进行校验，最终得到一个 16 位的校验码 C. 在原来 128 位随机密钥 K 后连接上 16 位校验码，构成

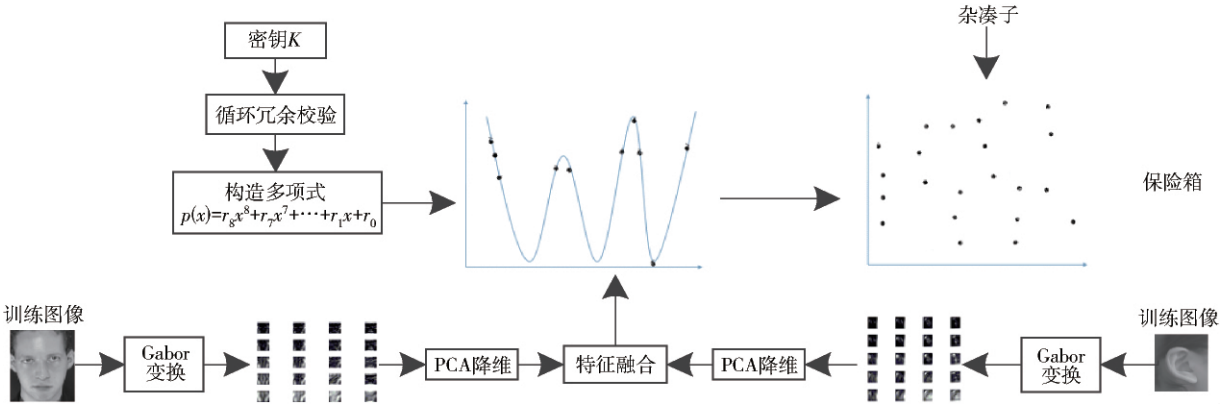

图 2　模糊保险箱模板加密流程图

Fig. 2　Template encryption diagram of the fuzzy vault

最终的码字,记为 K_C.

(2) 在有限域 $F(2^{16})$ 上,将 K_C 共 144 位二进制数分为 9 段,每段两个字节,从高位到低位分别记为 r_8, r_7, r_6, r_5, r_4, r_3, r_2, r_1, r_0. 根据这些值,构建出如下多项式:

$$p(x)=r_8x^8+r_7x^7+r_6x^6+r_5x^5+r_4x^4+r_3x^3+r_2x^2+r_1x+r_0. \quad (1)$$

(3) 由于人脸、人耳图像均使用 Gabor-PCA 方法进行特征提取,特征向量中特定位置的数值具有一定的意义,因此这种特征向量属于有序的数据集. 将融合特征模板数据通过上述构建的多项式 $p(x)$ 投影,就会得到如下点集:

$$\{[s_1,p(s_1)],[s_2,p(s_2)],\cdots,[s_i,p(s_i)],\cdots,[s_N,p(s_N)]\}.$$

其中, $[s_i,p(s_i)]=\{[s_{i1},p(s_{i1})],[s_{i2},p(s_{i2})],\cdots,[s_{ij},p(s_{ij})],\cdots,[s_{iL},p(s_{iL})]\}$, $i=1,2,\cdots,N$, $j=1,2,\cdots,L$, N 为所有注册模板的个数, L 为特征模板的维数, s_i 表示第 i 个特征模板, $p(s_i)$ 表示模板 s_i 中的每个分量在多项式 $p(\cdot)$ 上的投影. 保险箱中的真实点集即由这组数据构成.

(4) 在保险箱中添加杂凑点集 $(C,q(C))$,其中 C 为杂凑点向量, $q(C)$ 为其在多项式 $q(\cdot)$ 上的投影向量. 在本文中,为每个注册模板设定若干个杂凑子向量. 同时,为保证安全性,要求杂凑子向量的个数 $M\gg N$. 这些杂凑点的构造原则是在有限域 $F(2^{16})$ 中,但不能落在多项式上,即 $q(C)\neq p(C)$,并且与真实点有足够远的距离. 图 3 为真实点和杂凑点的分布示意图. 横轴表示特征模板的第一个维度,纵轴表示经过投影后的值. 圆圈表示真实点,星号代表杂凑子. 选取了 5 个真实点,每种颜色属于不同的类别,每个真实点附加 20 个杂凑子,同一颜色的表示为同一类的真实点与杂凑子. 为防止通过杂凑子推导出真实点,在这里杂凑子是随机分布的. 经过上述操作,密钥就被隐藏在保险箱中. 攻击者如果不能提供真实的特征点集,就很难从保险箱中获取密钥.

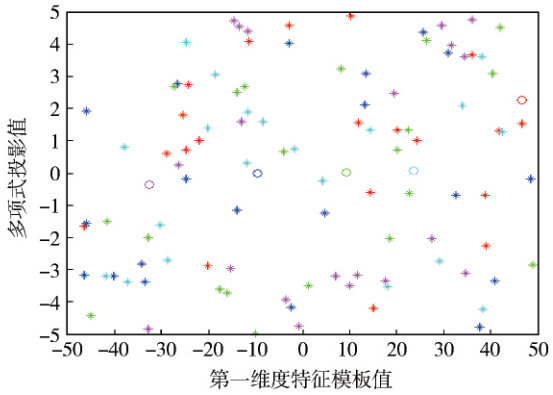

图 3　杂凑子与真实点的分布(圆圈为真实点,星号为杂凑子)

Fig. 3　Distribution of chaff points and vault points (circles are genuine points and asterisks are chaff points)

1.2　解密过程

之前的加密过程中,得到了模糊保险箱. 在解密阶段,对于待认证特征模板 t,如果 t 与注册模板 s 的大多数点重合,那么 t 的大多数点就会落在多项式 $p(\cdot)$ 上,使用纠错码方法,那么 t 就能重构出多项式 $p(\cdot)$,进而获取密钥 K^*. 如果 t 与 s 有相当大的比例不重合,那么重构出多项式 $p(\cdot)$ 是相当困难的. 解密过程的具体流程如图 4 所示.

为了重构多项式 $p(\cdot)$,至少需要特征模板中的 9 个点(因为 $p(\cdot)$ 为八次多项式). 为了从保险箱中获得至少 9 个真实点,需要注册模板和待认证模板中的元素进行逐个比对,获取候选点. 在比对过程中,需要设定阈值来判别待认证模板与保险箱中已加密模板是否属于同一类别. 在实验中,设定一个阈值 d_0,计算待认证模板与保险箱中注册模板的最小欧式距离,若距离小于 d_0,则认为是匹配上的点. 匹配完成之后,滤去了大部分的杂凑子,可以得到至少 9 个真实点,将获得的点集存储起来,记为 R,为下一步的恢复密钥做准备.

在加密阶段,密钥被分为 8 个 16 位的二进制串,并作为多项式的系数隐藏起来,所以在解密阶段要想

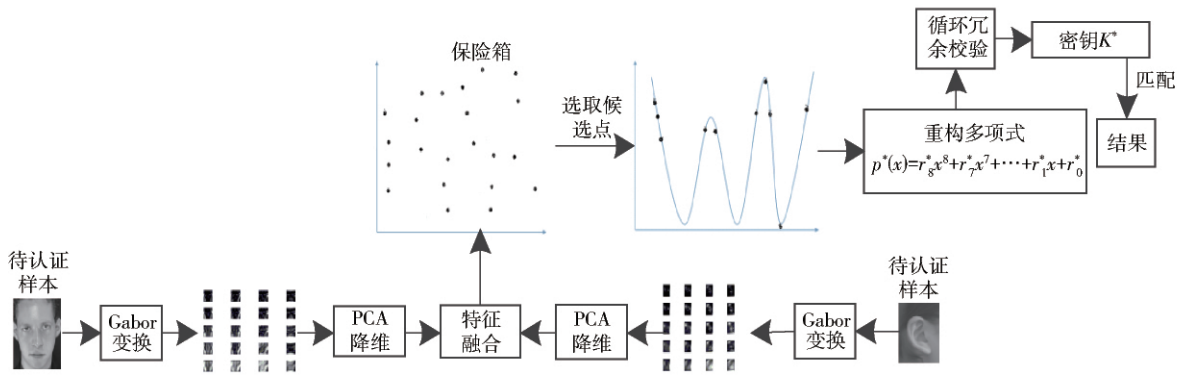

图 4　模糊保险箱解密流程图

Fig. 4　Decryption diagram of the fuzzy vault

恢复密钥，就得首先进行多项式的重构. 本文使用拉格朗日插值法进行多项式重构，在 R 中任取 9 个候选点，即为 (g_i, h_i)，$i = 1, 2, \cdots, 9$，其中 g_i 是从注册模板中选取的特征点，h_i 是其在多项式 $p(\cdot)$ 上的投影. 针对候选点，采取的拉格朗日插值法进行重构，如下所示：

$$p^*(x) = \frac{(x-g_2)(x-g_3)\cdots(x-g_9)}{(g_1-g_2)(g_1-g_3)\cdots(g_1-g_9)}h_1 + \frac{(x-g_1)(x-g_3)\cdots(x-g_9)}{(g_2-g_1)(g_2-g_3)\cdots(g_2-g_9)}h_2 + \cdots + \frac{(x-g_1)(x-g_2)\cdots(x-g_8)}{(g_9-g_1)(g_9-g_2)\cdots(g_9-g_8)}h_9 \tag{2}$$

化简上式，获得候选多项式为 $p^*(x) = r_8^* x^8 + r_7^* x^7 + \cdots + r_1^* x + r_0^*$. 接下来将 $r_8^*, r_7^*, \cdots, r_1^*$ 分别表示为 16 位字符串形式，然后将这 8 个字符串串联起来，得到一个 128 位的字符串，记为 $K^* = [r_8^* \| r_7^* \| \cdots \| r_1^*]$，然后将 K^* 进行 CRC−16 校验，获得其校验码 r'. 若校验码 $r' = r_0^*$，则表明 K^* 就是密钥，从而实现认证. 若校验码 $r' \neq r_0^*$，则说明选取的 9 个初始点不全是真实点，继续从 R 中选取点进行上述操作，直到获取满足条件的点集. 如果遍历 R 没有获得满足 $r' = r_0^*$ 的点集，则可判断认证失败，该用户为非法用户.

2　实验结果与分析

2.1　图像库简介

在实验中，我们使用 ORL 人脸库与 USTB 人耳子库 3 共同构成一个多模态图像库. ORL 人脸库包括 40 个人，每人 10 幅，共 400 幅人脸图像，存在表情、20° 以内轻微角度变化，如图 5(a) 所示. USTB 人耳子库 3 包括 79 人，每人 10 幅，共 790 幅图像，存在 20° 以内轻微角度变化，如图 5(b) 所示. 本文在 USTB 人耳子库 3 中随机挑选 20 个对象来与 ORL 人脸库中的 20 个对象进行组合，每人 5 幅图像进行训练，为每一张人脸图像配上一张人耳图像，作为一对样本. 实验结果采用识别率(genuine accept rate，简称 GAR) 和误识率(false accept rate，简称 FAR) 来评价.

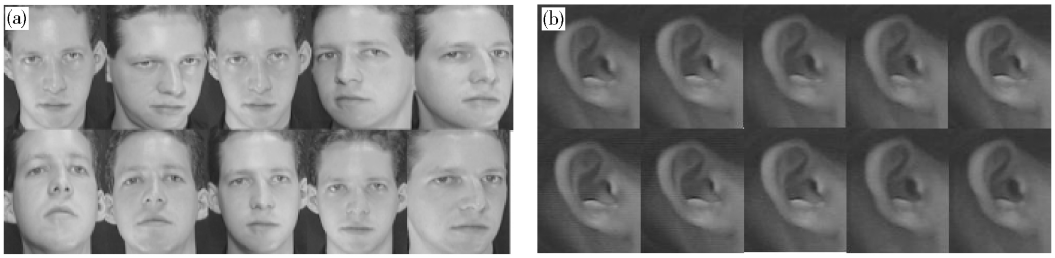

图 5　人脸图像及其对应的人耳图像. (a) ORL 人脸库示例；(b) USTB 人耳子库 3 示例

Fig. 5　Example images of the multimodal dataset: (a) ORL face dataset; (b) USTB ear dataset 3

2.2　人脸−人耳特征提取与融合

首先，分别对人脸和人耳源图像进行直方图修正，使得图像具有统一的均值和方差，同时在一定程度上消除光照的影响. 接下来利用 Gabor 小波变换[9] 来提取人脸和人耳不同尺度和方向的信息. 图 6 所示为一幅人脸图像在 5 个尺度、4 个方向上的 20 个幅值图谱. 将这 20 幅幅值图谱展开成向量并串联起来构成人脸图像对应的 Gabor 特征，由于其维度很高，所以进一步利用主元分析法进行降维，形成最终的特征模板.

因为获得的人脸 Gabor 特征和人耳 Gabor 特征是同质的，可以将两者在特征层进行融合[10]，生成融合特征模板. 设所得特征向量分别为 $\boldsymbol{s}_{\text{face}}$ 和 $\boldsymbol{s}_{\text{ear}}$，接下来对特征向量进行归一化处理：

$$\begin{cases} \boldsymbol{s}_{\text{face\_norm}} = (\boldsymbol{s}_{\text{face}} - \boldsymbol{\mu}_{\text{face}}) / \boldsymbol{\sigma}_{\text{face}}, \\ \boldsymbol{s}_{\text{ear\_norm}} = (\boldsymbol{s}_{\text{ear}} - \boldsymbol{\mu}_{\text{ear}}) / \boldsymbol{\sigma}_{\text{ear}}. \end{cases} \tag{3}$$

式中，$\boldsymbol{\mu}_{\text{face}}$ 和 $\boldsymbol{\mu}_{\text{ear}}$ 分别是注册样本集中人脸和人耳的均值向量，$\boldsymbol{\sigma}_{\text{face}}$ 和 $\boldsymbol{\sigma}_{\text{ear}}$ 分别为人脸和人耳的标准差向量. 采用特征积融合的方法，获得融合后的特征模板：

$$\boldsymbol{s}_{\text{fusion}} = \boldsymbol{s}_{\text{face\_norm}} \boldsymbol{s}_{\text{ear\_norm}}. \tag{4}$$

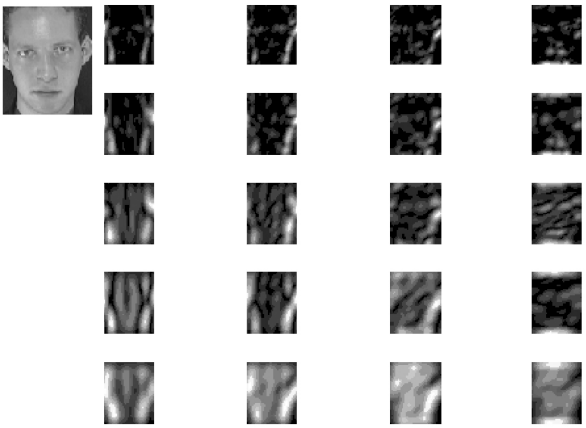

图 6　经过 Gabor 变换后的人脸幅值图谱

Fig. 6　Face magnitude representation after the Gabor wavelet transformation

2.3　认证性能

测试了人脸特征模板、人耳特征模板和融合特征模板在不同特征维数下的认证性能，正确识别率和误识率如表 1 所示(实验环境为 Window XP 操作系统，CPU Intel Core 2 Duo，2.16 GHz memory 2 Gb，Matlab

2012b).

表 1　不同特征模板维度下识别率和误识率的比较

Table 1　Genuine accept rate and false accept rate obtained under different template dimensions

特征模板维数	所用模态	识别率/%	误识率/%
15	人脸	76%	12%
	人耳	78%	9%
	人脸-人耳融合	81%	5%
20	人脸	90%	8%
	人耳	93%	6%
	人脸-人耳融合	95%	3%
25	人脸	92%	7%
	人耳	95%	6%
	人脸-人耳融合	96%	2%

从表 1 可以看出,随着特征模板维数的增加,识别效果越来越好,当维数达到 20 维时,识别率已经取得较好的效果. 另外,在相同的特征模板维度下,基于多模态特征融合模板的保护方法的识别率明显优于基于单模态人脸和单模态人耳模板的保护方法,并且误识率有了一定的降低.

3　结论

在特征融合和模糊保险箱的基础上,提出了一种人脸-人耳融合生物特征模板保护方法. 基于模糊保险箱算法的生物特征模板保护分为加密和解密两个阶段. 加密阶段将注册生物特征模板进行加密,转换成真实点集,并隐藏在杂凑点集中,真实点集与杂凑点集共同构成保险箱; 解密阶段将待认证生物特征模板通过保险箱提取密钥,并根据密钥进行认证. 在由 USTB 人耳库 3 和 ORL 人脸库构成的多模态图像库上的认证结果表明,该生物特征模板保护方案取得了较好的效果. 在下一步的研究中,将进一步优化加密算法和解密算法以缩短认证时间; 同时扩大实验样本的范围,减小小样本误差对实验的影响.

参　考　文　献

[1] Jain A K, Nandakumar K, Nagar A. Biometric template security. *EURASIP J Adv Signal Process*, 2008, 2008: 113

[2] Uludag U, Pankanti S, Jain A K. Fuzzy vault for fingerprints // *Proceedings of 5th International Conference On Audio- and Vedio-based Biometric Person Authentication*. New York, 2005: 310

[3] Nandakumar K, Jain A K. Fingerprint-based fuzzy vault: implementation and performance. *IEEE Trans Inf Forensics Secur*, 2007, 2(4): 744

[4] Lee Y J, Bae K, Lee S F, et al. Biometric key binding: fuzzy vault based on iris images // *Proceedings of International Conference on Biometric*. Seoul, 2007: 800

[5] Nandakumar K, Jain A K. Multibiometric template security using fuzzy vault // *Proceedings of the 2nd IEEE International Conference on Biometrics: Theory, Application and Systems*. Washington DC, 2008: 1

[6] Nagar A, Nandakumar K, Jain A K. Securing fingerprint template: fuzzy vault with minutiae descriptors // *Proceedings of the 19th International Conference on Pattern Recognition*. Florida, 2008: 1

[7] Mu Z C, Yuan L, Zeng H. *Biometric Identification Technology: Ear Automatic Recognition*. Beijing: Science Press, 2012
(穆志纯, 袁立, 曾慧. 生物特征识别技术: 人耳自动识别. 北京: 科学出版社, 2012)

[8] Liu H J, Zhang N T. Design of rapid CRC algorithm based upon table-lookingup methods. *Commun Technol*, 2002(4): 8
(刘会杰, 张乃通. 基于查表法的快速 CRC 算法设计. 通信技术, 2002(4): 8)

[9] Zhu J K, Vai M I, Mak P U. Gabor wavelets transform and extended nearest feature space classifier for face recognition // *Proceedings of the 3rd International Conference on Image and Graphics*. Hong Kong, 2004, 246

[10] Yazdanpanah A P. Faez K, Amirfattahi R. Multimodal biometric system using face, ear and gait biometrics // *Proceedings of the 10th International Conference on Information Science, Signal Processing and Their Application*. Kuala Lumpur, 2010: 251